ISSN 2704-8012

European Journal of Privacy Law & Technologies

Special issue (2020)

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

Special issue (2020)

Edited by Massimo Foglia

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in September 2020
www.ejplt.tatodpr.eu

PROCESSING PERSONAL DATA AND THE ROLE OF CONSENT

Shaira Thobani, University of Torino

Abstract:

Consent of the data subject is one of the leading bases to process personal data. However, its role and importance are strongly limited not only by other provisions of data protection law, but also by consumer protection rules. The essay will therefore focus on these limitations, which lead to some more general reflections on the interests at stake in data processing and on the legitimacy of a market of personal data.

Keywords: Personal data, Consent, Tying practices, Consumer law

1. Introduction

It is well known that most people, when asked, do seriously care about their data. However, it is also recognised that those same people, when required to take action to protect their data, do almost nothing in that respect. This discrepancy between attitude and behaviour when it comes to privacy is usually referred to as the 'privacy paradox' [1]. The explanations given to this phenomenon

[1] A. ACQUISTI-J. GROSSKLAGS, *Privacy and Rationality in individual Decision Making* (2005) 3(1) *IEEE Security & Privacy*, 26; S. KOKOLAKIS, *Privacy Attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon* (2017) 64 *Computers & Security*, 122; L. GATT-R. MONTANARI-I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali* (2018) *European Journal of Privacy Law & Technologies*, <http://www.ejplt.tatodpr.eu/Article/Archive/index_html?idn=2&ida=29&idi=-1&idu=-1> accessed 17 February 2020; N. GERBER-P. GERBER-M. VOLKAMER, *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior* (2018) 77 *Computers & Security*, 226.

are mainly related to the lack of information and cognitive biases of data subjects who, on the one hand, do not have access to all the relevant information regarding their data that would allow them to take an informed decision and, on the other hand, do not have the means to process the information they are given [2]. Moreover, the data subjects who consent to the processing of their information usually lack a clear perception of the value of such data and do not suffer from negative consequences that they can easily trace back to the processing. As a consequence, an individual confronted with the decision either to click on "I consent" or to read the privacy policy of a website will mostly prefer the former.

Notwithstanding this empirical evidence, the consent of data subjects is one of the main bases for processing personal data. Under the General Data Protection Regulation 679/2016 (as under previous directive 95/46/EC) processing is lawful if, among other conditions, "the data subject has given consent to the processing of his or her personal data for one or more specific purposes". Consent is not the only basis to lawfully process data. It is, however, the broadest one, as the other conditions require the processing to be undertaken for specific reasons while consent can be asked to process data for any purposes. Indeed, the widespread practice of requesting consent also seems to suggest that consent is one of the most commonly used bases for processing personal data. In practice, this may be related to the uncertainty surrounding some of the other bases for processing data, such as the legitimate interest clause: as this clause is not clear as to what amounts and what does not amount to a legitimate interest, controllers tend to ask for consent to ensure that the processing is lawful.

In spite of the importance attributed to consent, there are however other provisions that downsize its role. As we shall see in the following paragraphs, some of these limits stem from data protection law itself and others from consumer protection law. The role of consent shall therefore be assessed bearing in mind these restrictions.

2. The role of consent under data protection law

The GDPR itself, while putting consent in a prominent position on the one hand, does not seem to fully trust its suitability to protect the interests involved in data protection on the other. In the first place, it compels the controller to put in place certain measures to protect the interests affected by data processing even if the data subject has consented to the processing. In the second place, it

[2] D.J. SOLOVE, *Privacy Self-Management and the Consent Dilemma* (2013) 126 *Harvard Law Review*, 1880.

strictly regulates consent, prescribing it to meet stringent requirements. Finally, it excludes that in some cases the processing can be based on individual consent.

Firstly, in any case, even if the data subject has lawfully consented to the processing, the controller must not only put in place adequate security measures to preserve the integrity of the collected data, but he is also required to limit the risks deriving from the processing. The controller must indeed evaluate those risks and in certain cases perform a data protection impact assessment (art. 35 GDPR); if risks are serious and cannot be minimised, the controller shall stop *tout court* the processing. This clearly demonstrates that the processing, even if it has been consented to, may still be harmful: not only because individual consent is not completely reliable considering the cognitive biases affecting data subjects, but also because the risks in question concern not only the individual, but society more in general. As is well known, data protection regulation was born to address the risks stemming from technological development regarding, for instance, social control, discrimination, surveillance, social conformity, segregation and exclusion of minorities. These risks have a collective dimension and therefore cannot be tackled by individual consent only [3]. Therefore, consent does not exempt controllers from evaluating and minimising those risks.

As regards the requirements of consent, consent must be "freely given, specific, informed and unambiguous" (art. 4, lett. 11). Leaving aside for now the requirement of freedom of consent, the aim of the other requirements is doublefold. Firstly, it is to promote awareness of the existence and of the scope of the processing by the data subject: the data subject shall be aware that they are consenting to the processing (consent must be unambiguous) and they shall be aware of what they are consenting to (consent must be informed). The second aim is to limit what controllers can do with the data: even if the data subject consents, their consent shall not be too broad but must be referred to a specific purpose (consent must be specific).

Finally, consent cannot always be used as a legitimate basis for processing personal data: more precisely, consent cannot be invoked if the circumstances prevent it from being freely expressed. It is therefore necessary to examine the requirement that consent is *freely* given, as provided for by the GDPR. According to the Art. 29 Working Party, freedom of consent "implies real choice and control for data subjects", in the sense that "if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not

[3] A. MANTELERO, *Personal data for decisional purposes in the age of analytics: From and individual perspective to a collective dimension of data protection* (2016) 32 *Computer Law & Security review*, 238.

consent, then consent will not be valid"[4]. Therefore, for consent to be free, the data subject must have a real choice whether to give it or not. What does it mean to have a *real choice*?

In the first place, the choice is not *real* if there is a qualified imbalance of power between the controller and the processor[5]. This is the case, for instance, of public authorities or employers, who cannot rely on consent to process personal data of citizens or employees if they take advantage of their position to obtain consent. Therefore, an employer cannot ask its employees to consent to the processing of their personal data as a condition to continue being employed (provided, of course that those data are not necessary to perform the job, e.g. the work telephone number to call the employee when he is on duty: in this case the employer is entitled to process the data without the employee's consent). Another example could be that of hospitals or other healthcare facilities, which cannot ask patients to consent to the processing of their data as a condition to provide health care (here as well, provided that the data are not necessary to that end).

In the second place, the choice is not real if the data subject is forced to give consent in the sense that they do not have an alternative in order to have access to a good or service[6]. This is the issue of the so called *tying* practices, in which someone who provides a good or service makes the performance conditional on the users' consent to the processing of their personal data that are not necessary for the performance of the required service. Tying practices are at the core of the pervading business model of offering services for free (in the sense that no monetary price is asked in return) but upon request of personal data. Especially (but not only) in the online world, many services are offered provided that the users communicate some of their personal data when registering to the service and accept that the data generated while using the service are tracked and used by the service provider or by third parties.

Are tying practices prohibited by data protection legislation? The GDPR gives a nuanced answer, providing that "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of a contract" (art. 7, para. 4). Thus the GDPR does not prescribe a blanket prohibition, but states that tying consent to the processing to the performance of a contract shall be taken in "utmost account" when assessing the validity of con-

[4] Article 29 Working Party, *Guidelines on consent under Regulation 2016/679* adopted on 28 November 2017 as revised on 10 April 2018, WP259 rev.01, 5.

[5] *Ibidem* 6-7.

[6] *Ibidem* 8-10.

sent. To understand what this means it is useful to go back to the recommendations of the Art. 29 Working Party that the data subjects have a real choice. As said, there is no real choice if the data subject does not have an alternative to access a good or service without consenting to the processing of their personal data.

An alternative surely exists if the service provider offers two versions of the same service, one for free but asking users to consent to the processing of their data, and the other one without asking for consent [7]. In the latter case, the service provider can ask for a fee to use the service, provided, of course, that the price is reasonable: if the price were disproportionate to the service, users would not have a real choice not to consent to the processing.

The problematic question is whether an alternative exists if an equivalent service is offered on the market by another provider, who does not ask for consent to data processing. The Art. 29 Working Party denies this possibility [8] and some data protection authorities across Europe have taken a similar position as well [9]. The wording of art. 7 GDPR (which, as said, does not prescribe a blanket prohibition) suggests however a more flexible interpretation. Indeed, it seems reasonable to argue that if users are able to access an equivalent service without having to consent to the processing of their personal data, they do have a real choice [10]. Of course, the service must be equivalent: this excludes that those who offer a service in a quasi-monopolistic position (such as, e.g., Facebook and Google) can legitimately ask users to consent to the processing as a condition to use the service.

To summarise, data protection law restricts the role of consent by compel-

---

[7] *Ibidem* 9.

[8] *Ibidem* 9-10.

[9] See, e.g., the position of the Italian data protection authority (*Garante per la protezione dei dati personali*) in *Linee Guida in materia di attività promozionale e contrasto allo spam*, decision 4.7.2013, 330 and of the French authority (*Commission nationale informatique & libertés*), in *Projet de recommandation sur les modalités pratiques de recueil du consentement prévu par l'article 82 de la loi du 6 janvier 1978 modifiée, concernant les opérations d'accès ou d'inscription d'informations dans le terminal d'un utilisateur (recommandation «cookies et autres traceurs»)* 14.1.2020, art. 3. Instead, the British Information Commissioner's Office has taken a more nuanced position: while it recommends "that organisations do not make consent to marketing a condition of subscribing to a service unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent cannot be sought separately", it also stresses that it must be considered "whether there is a choice of other services and how fair it is to couple consent to marketing with subscribing to the service"; (*Direct marketing guidance*, version 2.3 of 6 March 2018, para. 66).

[10] This is the position taken by the first Italian court decision on the issue: Cass. 2.7.2018, 17278, in *Giur. It*., 2019, 3, 530, according to which tying practices are banned only when the service has no equivalents and is indispensable.

ling the controller to protect otherwise the rights and interests affected by the processing, by prescribing strict consent requirements and by excluding that in certain cases the processing of personal data can be based on consent. It is important to underline that it is one thing to provide for strict consent requirements, asking for consent to be unambiguous, informed and specific, and another thing to require that consent is free in the sense of limiting the possibility to base the processing on consent. In the first case, consent can be used as a legitimate basis for processing (and, therefore, data can be processed) provided that all information is given, that the data subject is aware of the processing and that the processing is limited to specific purposes. In the second case, the only way to abide by the requirement of freedom of consent is not to ask for it: as a consequence, in the absence of other conditions for the processing, data cannot be processed. The requirement of freedom of consent is therefore used as a way to limit the collection of personal data.

3. The role of consent under consumer law

In the previous paragraph we considered the limits to the role of consent from a data protection perspective. However, as consent to the processing of personal data is often asked for when offering a good or service, data subjects are at the same time consumers taking part in economic transactions and, as such, the role of their consent should also be evaluated from a consumer protection law perspective. There is no doubt that these are economic transactions, notwithstanding that in many cases the services in question are offered "for free": the economic value of personal data is well known and these services are offered without charging a fee precisely because there is an economic advantage deriving from the data collected when providing the service [11].

The European Commission has taken a stance on the issue, clarifying that data processing, together with advertising, often constitutes the main source of revenues of "data-driven business structures", as "[p]ersonal data, consumer preferences and other user generated content, have a 'de facto' economic value and are being sold to third parties". As a consequence, "if the trader does not inform a consumer that the data he is required to provide to the trader in order to access the service will be used for commercial purposes, this could be consid-

[11] While it is undisputed that personal data have economic value, doubts have arisen on how to measure it: see, eg, Organisation for Economic Co-Operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* (2013) *OECD Digital Economic Papers*, 220; G. MALGIERI-B. CUSTERS, *Priving privacy - the right to know the value of your personal data* (2017) 34 *Computer Law & Security Review*, 289, 294-297.

ered a misleading omission of material information" under directive 2005/29/EC (Unfair Commercial Practices Directive), especially under art. 7, para. 2 concerning misleading omissions [12]. The issue is one of transparency: traders cannot advertise their services as free if they ask for personal data in return for using the service. In order to abide by consumer protection law, it is therefore necessary to openly disclose the purposes for which consent to personal data protection is required and to make it clear to consumers that such purposes have an economic nature.

Transparency requirements under consumer protection law lead to a result that is partially similar to what is achieved applying data protection law [13]. The GDPR requires consent to be informed: this amounts to saying that service providers must be transparent to users on the use they make of the collected data. From a consumer protection point of view, the commercial practices shall be transparent while, from a data protection perspective, the data subjects' consent shall be informed: the result is the same, i.e. to clearly inform consumers/data subjects on the purposes and scope of the processing.

Consumer protection law also takes into consideration consent to data processing from another point of view. As said, providing a service asking not for a monetary price but for the consent to process personal data amounts to an economic transaction. Therefore, if consumers are involved, they deserve the protections provided for by consumer law for economic transactions. This aspect has been clarified by the European legislator in the recent Directive (EU) 2019/779 on certain aspects concerning contracts for the supply of digital content and digital services, which applies not only when the consumer "pays or

---

[12] European Commission, *Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices* SWD (2016) 163 final, 25.5.2016, 23-25. See also Case AT.39740, Google Search (Shopping), European Commission, 2017, 4444 final, decision of 27.6.2017, para. 158. The Italian competition authority has sanctioned this practices as unfair commercial practices: see, lastly, Case Facebook - condivisione dati con terzi, Autorità garante della concorrenza e del mercato, 29.11.2018, 27432 (the decision was later partially reversed by TAR Lazio, 10.1.2020, 260, that, however, confirmed that traders shall be transparent on the economic value of the consumers' data they collect).

[13] On the intertwines between personal data and consumer protection law see M. ROHEN, *Beyond consent: improving data protection through consumer protection law* (2016) 5(1) *Internet Policy Review*, <https://policyreview.info/node/404/pdf> accessed 17 february 2020; A. DE FRANCESCHI, *La circolazione dei dati personali tra* privacy *e contratto* (Napoli 2017), 101 ff.; N. VAN EIJK-C.J. HOOFNAGLE-E. KANNEKENS, *Unfair Commercial Practices: A Complementary Approach to Privacy Protection* (2017) 3 *European Data Protection Law Review,* 325; M. GRAZIADEI, *Collusioni transatlantiche: consenso e contratto nel trattamento dei dati personali*, in F. DI CIOMMO-O. TROIANO (eds.), *Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi* (Piacenza 2018), 367; C. GOANTA-S. MULDERS, *Move Fast and Break Things: Unfair Commercial Practices and Consent on Social Media* (2019) 8(4) *Journal of European Consumer and Market Law*, 136.

undertakes to pay a price", but also when the consumer "provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service" (art. 3) [14]. In both cases, consumers are entitled to the rights and remedies provided for in the Directive. The European legislator is careful to specify that this does not amount to considering personal data as a commodity that can be traded in return for a service [15] (instead, the extent to which this is legitimate is regulated, as we have seen, by data protection law), but only prescribes that, if in practice it happens that data are used for that purpose, then consumers shall be protected as if they had paid a price.

Summarising, consumer law tells us that, when consent to the processing of personal data is asked in the context of economic transactions, then consent shall be asked in a transparent way and data subjects are entitled to consumer protection. But consumer protection law cannot go beyond ensuring transparency and fairness in the processing. If the terms and conditions are clear enough and if consent is not acquired with unfair commercial practices, then consumers' consent to data processing can be legitimately asked. Instead, as we have seen, data protection law goes further in limiting the role of consent, excluding that under certain circumstances consent can be used as a legitimate basis to process data. Consumer law cannot go that far because, as it has developed in Europe, it cannot interfere with the economic content of market transactions: provided that the terms and conditions are clear and that consumers' choices have not been unduly influenced by unfair commercial practices, the "adequacy of the price and remuneration" is not subject to scrutiny (art. 4, para 2, Directive 93/13/EEC on unfair terms in consumer contracts). As we have seen, consumer law itself qualifies consent to the processing of personal data as a *de facto* remuneration, in order to protect consumers by ensuring the transparency of tying practices and by granting them remedies. By qualifying consent as a remuneration, and thus recognising its direct relevance for the economic content of the contract, it is excluded from scrutiny under consumer protection law. Instead, it is the task of data protection law to limit the role of consent and to prescribe when it can or cannot be used to collect data.

If consumer protection law does not allow a scrutiny on the economic conditions of the transactions in which personal data are involved, some doubts have

[14] On the issues raised by the Directive see A. DE FRANCESCHI (ed.), *European Contract Law and the Digital Single Market* (Cambridge 2016).

[15] Whereas 24 of the Directive. This clarification follows the concerns raised by the European Data protection Supervisor on the use of personal data as counter-performance: *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14.3.2017, 6-11.

been raised on whether it is possible to perform such a scrutiny under competition law. The question has emerged as an issue of abuse of dominant position: can a company with market dominance ask its users to consent to the processing of their personal data as a condition to access the service? [16] Here, once again, the answer seems to be negative, at least as argued by the German court, that for first in Europe addressed this specific issue [17]. Indeed, even if it is taken for granted that a dominant undertaking cannot ask for consent because consent would not be free (as users as have no other option to access an equivalent service without consenting to the processing) under data protection law, this does not imply that this conduct impairs competition and therefore needs to be sanctioned under competition law as well. Firstly, such sanction only applies if it is demonstrated that the business model of asking for data in return for a service would not be adopted in a competitive market: it is fully possible that such a business model is so widespread because of the cognitive limitations of data subjects and has nothing to do with the abuse of a dominant position. Secondly, because it needs to be demonstrated that this conduct has a negative effect on competition: if, on the one hand, users are not prevented from using other services as a result of the request to consent to the processing of their data and, on the other hand, other businesses are not prevented from collecting personal data themselves, then this does not seem to be the case. In other words, if a dominant undertaking infringes the law, this infringement will be relevant under the body of law in question, but it will not necessarily amount to a competition problem. It remains to be seen how the issue will be addressed by other European authorities and judges.

4. Conclusions

Having briefly seen the limits to the role of consent stemming from different sources, we can return to some general remarks on the role of consent to the processing of personal data.

---

[16] The question was given a positive answer by the German competition authority: Case B6-22/16, Bundeskartellamt, 6.2.2019. However the decision was later reversed by Case VI-Kart 1/19 (V), OLG Düsseldorf, 26.8.2019. The case regarded Facebook's data policy, which the Bundeskartellamt found abusive in the part that made the use of the social network conditional upon users' extensive consent to process the personal data generated while using external services.

[17] Case VI-Kart 1/19 (V), OLG Düsseldorf, 26.8.2019. On the matter see R. PODSZUN, *Regulatory Mishmash? Competition Law, Facebook and Consumer Protection* (2019) 2 *Journal of European Consumer and Market Law*, 50; G. COLANGELO, *Facebook and the Bundeskartellamt's Winter of Discontent* (2019) *Competition Policy International*, <https://www.competitionpolicyinternational.com/facebook-and-bundeskartellamts-winter-of-discontent/> last accessed 17 February 2020.

Firstly, why, in spite of the aforementioned limits, does the European legislator still give it such a prominent role? A possible reason of the importance attributed to consent may lie in the way data protection has evolved in Europe. The right to the protection of personal data has been developed in the fundamental rights scenario and has been framed as a fundamental right by the UE charter of fundamental rights (art. 8)[18]. The European legislator has therefore shaped data protection as the subject of an individual right, thus drawing it to the realm of personality rights, which are, indeed, rights of the individual person. The underlying assumption is that data pertain to the individual they refer to and, therefore, individual consent is needed to process them. In other words, even without adopting an outright proprietary model with regard to personal data, if the protection of personal data is the subject of an individual right, then the consent of the right's holder is necessary for intrusions to be legitimate and, therefore, for the data to be processed.

Secondly, as we have seen, in spite of this importance, the European legislator is well aware of the weak effectiveness of consent to protect the interests involved in data processing and thus sets forth strict limits to the role of consent. What are the reasons of these limitations? At first sight, the reason lies in the protection of the individual data subject or consumer. This can be read as a response to the privacy paradox: as data subjects have limited rationality when it comes to protecting their data, the law steps in to protect the individual, both by providing for conditions of transparency and, in some cases, by limiting *tout court* the processing. Under this perspective, consent is not adequate because the individuals are not in the condition to give a fully aware consent. However, there is also another reason why consent is limited, which has to do, not with the protection of the individual, but with the protection of society. As we have seen, in some cases consent (even if it is fully informed, specific and there is no qualified power imbalance) cannot constitute a legitimate basis for processing, meaning that data cannot be processed: this is the case when there is no alternative to access an equivalent good or service. This leads to a direct limitation to consent, but indirectly it limits the possibility to process data in itself. The purpose of such a limitation is not only the protection of the individual (who is usually not directly affected by the processing of big data), but is the protection of society from the risks that the mass processing of personal data poses to the community: as mentioned, these are indeed the main risks that data protection

[18] S. RODOTÀ, *Data Protection as a Fundamental Right*, in S. GUTWIRTH-Y. POULLET-P. DE HERT-C. DE TERWANGNE-S. NOUWT (eds.), *Reinventing Data Protection* (Berlin 2009), 77; M. TZANOU, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right* (2013) 3(2) *International Data Privacy Law*, 88; G. GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Berlin 2014).

regulation at first intended to address. Under this perspective, consent (even if it is given by someone who is perfectly aware of what they are doing) should have no role as the interests at stake are not those of the individual. Individual consent is just not the right tool to address these issues because under this perspective the aim is to limit the collection of data in order to protect society more in general.

It can be doubted, however, that limiting personal data processing under data protection law is always the right tool to address all of these problems. Taking the example of discrimination (which is one of the main risks associated with data protection), if we fear that data processing could lead to discriminate parts of society, it is clear that the decisions regarding the processing cannot be left to the consent of individual data subjects. However, it can be doubted that data protection law is the right tool to address the issue. If the aim is to prevent discrimination, it is necessary in the first place to specify what the discriminatory results to forbid are: however, this is the domain of anti-discrimination law, not of data protection law. Put another way, if the aim is to prevent discrimination, using data protection law to limit the collection of personal data risks to lead to a blanket prohibition to the processing and prevents a transparent discussion on what are the discriminatory results to forbid. Therefore not only the role of consent, but also the role of data protection law should be reassessed considering whether other bodies of law are better suited to address the risks stemming from data processing.

This leads to a final conclusion. When assessing the role of consent, it should always be borne in mind what the protected interests are and what the final results that the limits to the role of consent lead to. The debate on the role of consent often focuses on whether it amounts or not to a contract and, therefore, on whether data can be considered as a tradeable commodity that can circulate by means of the data subjects' consent [19]. Due to reasons that regard not only the protection of individuals, but the protection of society more in general, the legislator can decide to forbid the "trade" of personal data by limiting the role of consent and prohibiting tying practices. This prohibition can be read as a means to protect the fundamental right to data protection. Under this perspective there is no space for consumer and competition law, which need a market to

[19] On the issue of using personal data as counter-performance see C. LANGHANKE-M. SCHMIDT-KESSEL, *Consumer data as consideration* (2015) 6 *Journal of European Consumer and Market Law*, 218; A. DE FRANCESCHI, *La circolazione dei dati* (fn 13) 67 ff.; A. METZGER, *Data as Counter-Performance: What Rights and Duties do Parties Have?* (2017) 8 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 1; G. RESTA-V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ*., 2018, 411, 436 ff.; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno,* in *Il diritto dell'informazione e dell'informatica*, 2018, 4-5, 689.

regulate, as, simply put it, there is not market (as a market of personal data is forbidden). However, data protection law aims at protecting not only the fundamental right to data protection, but also the free movement of personal data (art. 1, GDPR): excluding from this protection the processing of data for economic purposes (and, therefore, the possibility to develop a market of personal data) would mean to exclude a significant part of the interests that the free movement of personal data refers to. Indeed, the GDPR does not clearly forbid tying practices (art. 7, para 4) and this is not by chance: the rule in question was widely discussed during the preparatory works and a previous proposal providing for a blanket prohibition was discarded [20]. Therefore, as data can be traded (even though under the limits that we have previously seen), consumer and competition protection problems do arise and cannot be ignored: it is for the benefit of data subjects/consumers to acknowledge this openly and to put in place the necessary safeguards. Instead of denying the existence of a market which the law does not forbid, it is better to regulate it using all the available and relevant tools.

[20] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report 17 December 2012, 2012/0011(COD), amendment no 107, where the Parliament proposed to add the following para. to art. 7: "The execution of a contract or the prevision of a service may not be made conditional on the consent to the processing or use of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1)(b)". The position expressed in this work is not however commonly accepted at the European level: the Art. 29 Working Party firmly excludes that data can be used as a counter-performance to access a good or service: *Guidelines on consent* (fn 4) 8. See also, in the same direction as the Working Party, J.P. ALBRECHT, *The EU's New Data Protection Law - How a Directive Evolved Into a Regulation* (2016) 17(2) *Computer Law Review International*, 33, 36.